Amendments to the Claims

Please amend Claims 1, 8, and 15, as follows;

1.   (Currently Amended) A single sign-on authentication system, comprising:

an authentication component that determines whether a user is authenticated, and, if it is determined that the user is authenticated, generates a connection request;

an interface component that receives the connection request from the authentication component, the connection request including an identifier ~~associated with~~ identifying the authentication component and entitlement information associated with the user[[;]]_, wherein the interface component compares the received identifier identifying the authentication component with an expected identifier associated with the authentication component and, if they match, makes the entitlement information available to a ~~server~~ request processor associated with the interface component,

wherein the ~~interface component is connected to a~~ request processor is configured to determine one or more resources accessible by the authenticated user, based at least in part on the entitlement information.

2.   (Original) The single sign-on authentication system of claim 1, wherein the entitlement information is different from information used to authenticate the user.

3.   (Original) The single sign-on authentication system of claim 1, wherein the identifier includes an Internet Protocol (IP) address.

4.   (Original) The single sign-on authentication system of claim 2, wherein the authentication component determines the entitlement information based on the information used to authenticate the user.

5. (Original) The single sign-on authentication system of claim 4, wherein the information used to authenticate the user includes one or more of a user identifier and a password.

6. (Original) The single sign-on authentication system of claim 1, wherein the entitlement information is contained in a header portion of a data packet.

7. (Original) The single sign-on authentication system of claim 1, wherein the connection request is sent as an HTTP request.

8. (Currently Amended) A method for enabling an authenticated user to connect to a server in a computer network, comprising:

authenticating a user based on authentication information provided by the user to an authentication component;

receiving a connection request from the authentication component for the authenticated user, the connection request including an identifier ~~associated with~~ identifying the authentication component and entitlement information associated with the user;

comparing the received identifier identifying the authentication component with an expected identifier associated with the authentication component;

making the entitlement information available to a request processor associated with the server, only if the result of the comparison is a match, and

determining one or more resources accessible by the authenticated user, based at least in part on the entitlement information.

9. (Previously Presented) The method of claim 8, wherein the entitlement information is different from the authentication information.

10. (Original) The method of claim 8, wherein the received identifier includes an Internet Protocol (IP) address.

11.   (Previously Presented) The method of claim 9, wherein the entitlement information is determined based on the authentication information.

12.   (Previously Presented) The method of claim 11, wherein the authentication information includes one or more of a user identifier and a password.

13.   (Original) The method of claim 8, wherein the entitlement information is contained in a header portion of a data packet.

14.   (Original) The method of claim 8, wherein the connection request is sent as an HTTP request.

15.   (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable on the machine to perform method steps for enabling an authenticated user to connect to a server in a computer network, the method steps comprising:

authenticating a user based on authentication information provided by the user to an authentication component;

receiving a connection request from the authentication component for the authenticated user, the connection request including an identifier associated with identifying the authentication component and entitlement information associated with the user;

comparing the received identifier identifying the authentication component with an expected identifier associated with the authentication component;

making the entitlement information available to a request processor associated with the server, only if the result of the comparison is a match, and

determining one or more resources accessible by the authenticated user, based at least in part on the entitlement information.